UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/389,540	09/03/1999	LAWRENCE SMITH	105.0163US1	5546

21186 7590 10/01/2003

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	**PAPER NUMBER**
2131	6

DATE MAILED: 10/01/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/389,540	Applicant(s) SMITH ET AL.	
	Examiner Michael R Vaughan	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-16 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-16 is/are rejected.

7)☒ Claim(s) 7 is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 03 September 1999 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 4-5 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

Detailed Action

Claims 1-16 have been examined and are pending.

Claim Objections

Applicant is advised that should claim 6 be found allowable, claim 7 will be objected to under 37 CFR 1.75 as being a substantial duplicate thereof. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Benson (EP 936,530 A1).

As per claim 1, Benson teaches:

A virtual smart card server [57];

Storage connected to the virtual smart card server, which includes a plurality of smart card [0013];

Virtual smart cards (hereinafter VSC) are associated with a user [0013];

VSC include a private key [0007].

Benson teaches all of the limitations of claim 1 except expressly teaching that the authentication module is separate from the server and called by a different name. Benson teaches that the virtual card server (hereinafter VSC server) handles not only maintaining the database of VSC but also authentication. Because the server is all handled in software, any instance of the server could be in charge of the authentication and called by another name such as its function name. Therefore, it would have been obvious to modify the teachings of Benson by giving another name to the function that authenticates the VSC. The authentication module (agent) must in fact communicate with the VSC server in order to maintain the record of who is currently using their VSC. Hereafter the agent will be considered as part of the VSC.

As per claim 2, Benson teaches that the VSC interfaces with applications [0017].

As per claim 3, Benson teaches that the VSC performs encryption [0037] in response to applications [0023-0024].

As per claim 4, Benson teaches the VSC digitally signs a keyfile [0044].

As per claim 5, Benson teaches the VSC stores all of the protected information including key management [0025] in response to applications [0023-0024]. Benson teaches that a channel is established using key management functions [0036-0037]. It is therefore inherent that a channel is establishment after an application has detected the use of a VSC and must authenticate the VSC with the server.

As per claim 6 and 7, the examiner supplies the same rationale for the motivation as recited in the rejection of claim 1 to modify the teachings of Benson.

As per claim 8 and 9, Benson teaches that the VSC server communicates with the VSC over a transport layer [0036]. Benson also teaches that the VSC server communicates over the Internet [0024]. Therefore it is inherent that the VSC server uses TCP/IP to communicate with its clients because it uses a transport layer over the Internet.

Claims 10 –16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Benson in view of Handbook of Applied Cryptography (HAC hereinafter).

As per claims 10, 11, and 12, Benson teaches a method of authenticating users using a one time random password, which is encrypted and later decrypted [0049-0050]. If the random password can be decrypted in a reasonable amount of time, the user is authenticated [0050]. Benson teaches this authentication method using a symmetric key system. Benson fails to teach an authentication method using public/private keys and the use of a digital certificate. HAC teaches an asymmetric authentication method whereby the users are given a pair of keys, one public and one private (pg. 559-560). Also HAC teaches the use of a digital certificate to further authenticate the public key of a user (pg. 560). HAC teaches that the digital certificate must not be revoked (by checking a CRL) in order to pass validation (pg. 560 and pg. 576 – 577). The digital certificate is used to validate and obtain the public key of the authenticating user, which is used to decrypt data that was encrypted with the private key. One of ordinary skill in art would know that the private key could encrypt the one time random password. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of HAC into the system of Benson because it would allow two parties to authenticate by means of a trusted authentication protocol. Therefore the server would know that the user is legit because it can verify this by means of a trusted authority (HAC pg. 560).

As per claim 13, Benson's method is implemented in software and therefore it is inherent that a computer executes the program code necessary to carry out the method's steps [57].

As per claim 14, Benson teaches an authentication server [57] which stores keys and other important data such as digital signatures [0025-0026], which are associated to users [0025]. Benson teaches a host system whereby the server handles the authentication. Benson teaches that other components facilitate the transferring of data between the application and the server ([0023] and FIG. 1). The authentication server must in fact communicate with the other system components in order to maintain the record of who is currently using the VSC. Benson is silent in disclosing that a client signs a digital signature. The server does keep record of digital signatures. HAC teaches that challenge-responses may be performed by digitally signing the challenge to prove knowledge of a private key (pg. 403). One who proves knowledge of a private key must also know the public key of the pair. It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of

HAC into the system of Benson because the authentication server stores digital signatures and by signing challenges, the result could then be compared to the stored signatures to prove a that a user was using his/her own public key. Also HAC teaches the use of a digital certificate to further authenticate the public key of a user (pg. 560). The use of digital signatures and proving them are ways to ensure that users are whom they say they are.

As per claim 15, Benson is silent in disclosing that users have role-based access control. Having role-based access control makes a system able to have users that do not all have the same permissions and access to the same resources. Such is the case with most networks today. Some users have more permissions and are able to access more of the systems resources. Therefore, a network would want a way of differentiating between users based on the level of access. HAC teaches each resource has a list of identities associated with it (pg. 387). In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of HAC within the system of Benson because it would allow the system to allocate certain resources to particular users upon authenticating the user. This is one reason why it is pertinent that the system can stop users pretending to be someone else from entering the system.

Benson fails to teach that authenticating is logged. HAC teaches that authenticating is one motivation to allow resource usage to be tracked to identifiable entities (pg. 387). In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of HAC within the system of Benson because it would allow the system to keep a log of all who try to authenticate the system. The log can be analyzed to see which users are abusing the system or whose identity has been stolen.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US Patents

6,233,341 Riggins

5,347,580 Molva et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

MV
Michael R Vaughan
Examiner
Art Unit 2131

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100